Heliyon 5 (2019) e02855

Contents lists available at ScienceDirect

Heliyon

journal homepage: www.cell.com/heliyon

Research article

Cyber security education is as essential as "the three R's"

Isabella M. Venter [a,*], Rénette J. Blignaut [a], Karen Renaud [b,d,e], M. Anja Venter [c]

[a] University of the Western Cape, South Africa
[b] Abertay University, Dundee, Scotland, UK
[c] University of Cape Town, South Africa
[d] Rhodes University, Grahamstown, South Africa
[e] University of South Africa, South Africa

ARTICLE INFO

Keywords:
Computer science
Education
Gendered cyber-crime
Smartphone
Education
Cyber security
Gender

ABSTRACT

Smartphones have diffused rapidly across South African society and constitute the most dominant information and communication technologies in everyday use. That being so, it is important to ensure that all South Africans know how to secure their smart devices. Doing so requires a high level of security awareness and knowledge. As yet, there is no formal curriculum addressing cyber security in South African schools. Indeed, it seems to be left to universities to teach cyber security principles, and they currently only do this when students take computing-related courses. The outcome of this approach is that only a very small percentage of South Africans, i.e. those who take computing courses at university, are made aware of cyber security risks and know how to take precautions. In this paper we found that, because this group is overwhelmingly male, this educational strategy disproportionately leaves young South African women vulnerable to cyber-attacks. We thus contend that cyber security ought to be taught as children learn the essential "3 Rs"—delivering requisite skills at University level does not adequately prepare young South Africans for a world where cyber security is an essential skill. Starting to provide awareness and knowledge at primary school, and embedding it across the curriculum would, in addition to ensuring that people have the skills when they need them, also remove the current gender imbalance in cyber security awareness.

1. Introduction

In 1818, The Lady's Magazine included an article on "The Three R's" (reading, writing and arithmetic) (Percy and Timbs, 2019). Schools today still teach these foundational skills but also teach many more (Nias et al., 2005). Towards the end of the 20th century, information and communication technologies (ICTs) started to pervade daily lives, such that ICTs have now become an infrastructural essential on a par with electricity and water (Carr, 2003). In addition to the three R's, schools and higher education increasingly also teach ICT skills to children from a very young age. The United Kingdom (UK), for example, proposes curricula for early education to include Information and Communications Technology as a foundational skill (Education and Training Foundation, 2019). There are also moves to ensure that children are taught about online *safety* (Sutton, 2011) and how to spot fake news (Cockburn, 2019).

ICT use is now intertwined with Internet use. It then follows that anyone using the Internet, whatever their age, also needs to know how to secure their devices because forewarned is forearmed (Renaud et al., 2016). Safety and security are semantically different concepts (Waldron, 2006) requiring different kinds of knowledge and skill sets. Smartphone users, of all ages, should know that their phones are vulnerable to attack, and also know how to improve device security. Because education is at the heart of security awareness and capability (Siponen, 2001), it is imperative for cyber security education to reach all of society and all ages.

Cyber security education has two elements: first people need to become aware of the need to take precautions, and then teachers need to impart the skills they require to take the required precautions. We plan to assess awareness, as an essential prerequisite to mastering cyber security skills. We focus on assessing levels of cyber security awareness of university students in South Africa, as developing country citizens i.e. the "outcome" of the wider South African cyber security educational approach. Moreover, we explore whether the extant awareness levels exhibit the same gender imbalance as that evidenced in other societal

* Corresponding author.
E-mail address: iventer@uwc.ac.za (I.M. Venter).

https://doi.org/10.1016/j.heliyon.2019.e02855
Received 24 April 2019; Received in revised form 11 August 2019; Accepted 13 November 2019

domains in South Africa (Langen, 2005; Choi and Ting, 2008; Chinyamurindi and Louw, 2010).

We chose to focus on *smartphone* cyber security in South Africa, for three reasons:

- The first is that cyber-attacks increase year on year (Fowler, 2016), and developing countries are not exempt (Olapido, 2015). Cyber criminals, finding that large organisations are getting better at cyber security and are therefore becoming more difficult to compromise, have now turned their attention to easier targets: small businesses and home computer users (Krebs, 2017), both of whom do a great deal of their computing on their smartphones (Asadullah Khaskheli and Bhuiyan, 2017).
- The second reason is that smartphone ownership is increasing globally, offering an attractive attack surface that hackers can use to target the unwary or unprotected (Mayer, 2014). Smartphone adoption has increased beyond expectations but, unfortunately, so have security vulnerabilities. A lack of education and awareness is contributing to the growing cyber-security problem (Hanus and Wu, 2016). South African smartphone ownership was 51% in 2018 (Pew Research Centre, 2018), which is higher than global computer ownership (Newzoo, 2017), meaning that South Africans might be even more vulnerable to smartphone-enabled attacks than citizens of other countries.
- The third reason is that South African children own and use smartphones at increasing rates. Businesstech reported that 80% of secondary South African school pupils owned a smartphone in 2017 (Businesstech, 2019), and Porter (2016) reported that 51% of primary South African school pupils owned mobile phones. Because South African adolescents and youth are the first adopters of new mobile technologies (Beger and Sinha, 2012) and South African University students are heavy users of smartphones (North et al., 2014), we cannot wait until adulthood to raise awareness of security issues and ensure that people have the requisite security-related skills.

South African schools and universities are starting to incorporate cyber security into many of their educational programmes (Kortjan and von Solms, 2014; von Solms and von Solms, 2014). According to Dlamini & Modise, the South African government is investing in cyber security efforts to help improve cyber resilience (Dlamini and Modise, 2013). However, there does not seem to be a formal across-the-board curriculum for cyber security (De Lange and von Solms, 2012). It cannot be assumed that all South Africans' awareness of cyber security issues is being improved by these efforts. Any educational endeavour needs routinely to assess its impact, so that interventions can be refined and improved and made as effective as possible. We thus assess the impact of the South African approach to raising cyber security awareness.

The main contribution of this paper is to:

1. emphasize the need to treat cyber security (and not merely ICT) as a foundational skill, alongside other basic skills throughout the educational system—together with the basic "three R's".
2. highlight the impact of the current South African approach to cyber security education i.e. rendering young women more vulnerable to cyber-attacks, and thereby exacerbating the gender imbalance in South African society.

We consider related research in Section 2 before explaining our research methodology in Section 3. Section 4 presents our results, with Section 5 discussing and reflecting on them. Section 6 concludes.

2. Related research

The world is on the brink of a new revolution: the Fourth Industrial Revolution. According to the World Economic Forum (World Economic Forum, 2017a), this new technological revolution will fundamentally change the way people live and work. This change, if not embraced and anticipated, could minimize, or even derail, the potential it has for development and innovation in developing countries.

According to ITU, Internet users (worldwide) increased from 1991 million in 2010–3385 million in 2016 (ITU, 2018a). Among these users, young people (aged 15–24) are the most prominent users (71%), a high number given that only 48% of the total world population uses the Internet.

2.1. Regional differences

As shown in Figure 1, there is a distinct within-country digital divide in Africa.

In developing countries, the Internet is accessed mostly via mobile phones (Statista, 2019). As many as 81% of South African households in metropolitan areas only use mobile phones at home (see Figure 2). Although Internet usage increased from 30% of the world's population in 2010 to 47% of the world's population in 2016 (ITU, 2018b), in Africa only 25% of the African population used the Internet in 2016. In November 2018 the average cost of 1GB of mobile data in South Africa was $7.19. Cable.co.uk[1] places South Africa 143 out of 230 countries in terms of its mobile data cost. The most expensive country was Zimbabwe (with an average of $75.20 per GB) and the cheapest was India (with an average of $0.26 per GB).

A high proportion of South Africans only access the Internet at places where they can access free Wi-Fi because data costs in South Africa (compared to other BRICS countries) are prohibitive (see Figure 3). Chigona et al. indicated, in an article about people living in disadvantaged communities in the Western Cape, that they visited libraries with Wi-Fi access at least once a week and primarily used this library service to do research and access social media sites (Chigona et al., 2016).

2.2. Gender differences in Science, Technology, Engineering or Mathematics

According to the World Bank report, the Internet usage gender gap in Africa has increased since 2013, and not decreased as in other regions (The World Bank, 2016).

The first step in moving towards gender equality is to find areas where such inequality is occurring. Only then can targeted efforts be made to address and reduce inequalities. It is clear that women, especially young girls, still face inequalities in terms of computer and Internet access (The World Bank, 2016) (Livingston et al., 2017), as demonstrated in Table 1. It is interesting to note that the only place where the proportion of women using the Internet is greater than that of men (ITU, 2018b) is in the Americas.

Women who study at tertiary institutions, in both advanced and developing countries, are less likely than men to choose a career in Science, Technology, Engineering or Mathematics (STEM) and are paid less than their male counterparts in the same positions once they qualify. In the United States, less than 25% of STEM positions are filled by women and, for every dollar a man earns in this field, a woman earns only 86 cents (Beede et al., 2011). The majority of women with a STEM degree (56%) prefer to work either in education or health care (UNESCO Education Sector, 2017). In 2017, a report by the United Nations Educational Scientific and Cultural Organisation (UNESCO) reported that only 35% of students graduating world-wide in STEM fields are women (UNESCO Education Sector, 2017).

It is important to create opportunities for women to "*increase the pipeline*" of potential employees in the technology industry. Currently, only 16% of graduates in computer science in the United States (US) are women, with only 18% filling "*tech roles*" in Silicon Valley (World Economic Forum, 2017b). It is estimated by Girls Who Code (WCD) (a

[1] https://www.cable.co.uk/mobiles/worldwide-data-pricing/.

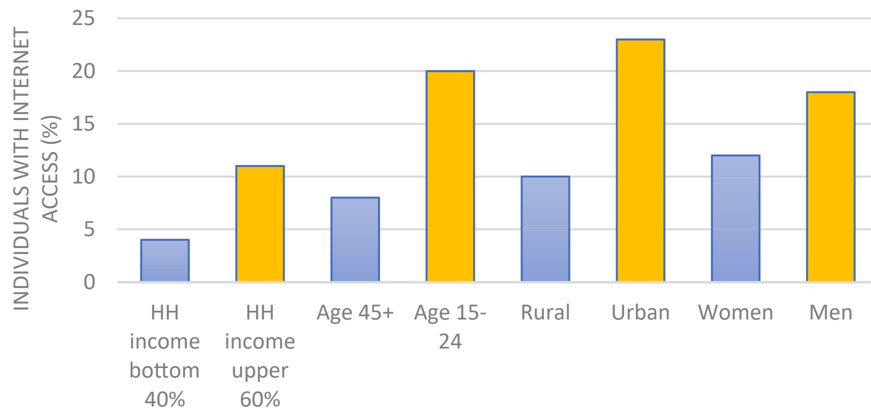

Figure 1. Within country digital divide in Africa (HH = Household) (The World Bank, 2016, p. 9).

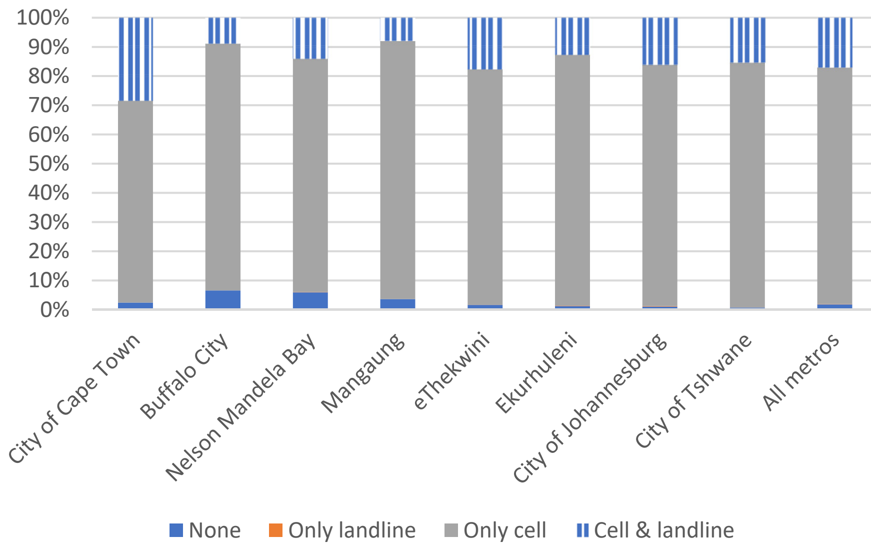

Figure 2. Households with a functional landline and cellular phone (Stats South Africa: Household Survey,2015).

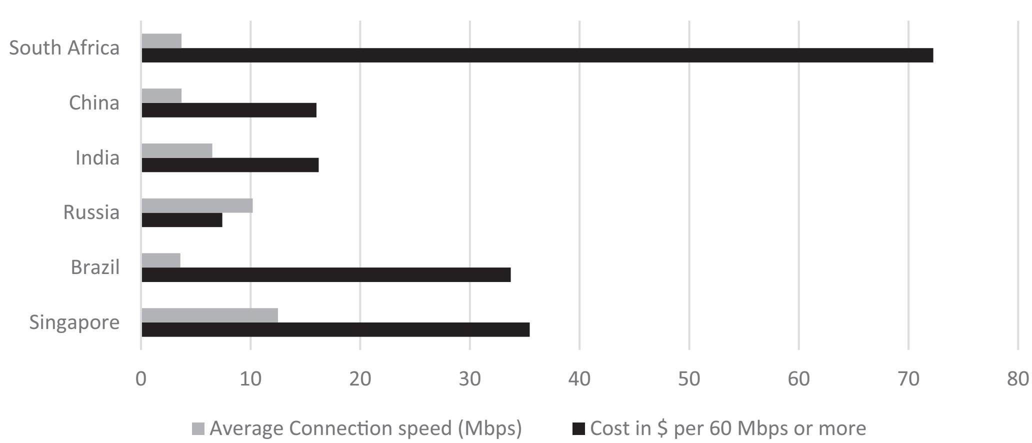

Figure 3. Cost and speed comparison: $ per Mbps (Numbeo, 2018) (Akamai Technologies, 2017)[2].

non-profit organisation that raises interest in technology sector careers) that women will hold only 3% of "*tech jobs*" in the US by 2020 (World Economic Forum, 2017b). In sub-Saharan Africa, the digital gender divide is even more pronounced, with fewer women than men completing tertiary education, owning a cell phone or accessing the Internet (Alozie and Akpan-Obong, 2017).

According to the World Bank report, a gender gap exists at home and in the educational system even before girls enter university—with only

[2] Singapore is not one of the BRICS countries but was included in the original Figure we sourced.

Table 1. Internet penetration in 2017 by gender (ITU, 2018b).

Type of Region	Women	Men	Gap	Total
Developed	79.9	82.2	2.3	81
Developing	37.5	44.7	**7.2**	40
Least Developed	14.1	21	**6.9**	18
World	44.9	50.9	6	47
Africa	18.6	24.9	6.3	22
Arab States	39.4	47.7	8.3	44
Asia and Pacific	39.7	47.9	8.2	42
CIS	65.8	69.8	4	68
Europe	76.3	82.9	6.6	80
The Americas	66.7	65.1	-1.6	66

5% of 15-year-old girls (compared to 18 percent of boys) in Organisation for Economic Co-operation and Development (OECD) economies considering a career in STEM (Organisation for Economic Co-operation and Development, 2009). It is important to address gender stereo-typing early on, and to encourage girls to believe that they are able to excel in this field and to provide incentives for recruitment and the graduation of women in these fields. It is also important that the work environment be gender-friendly (The World Bank, 2016; European Platform of Women Scientists, 2016).

It is appropriate to pause for a moment to offer a disclaimer on how the authors used the concept of "gender" in this paper. While the authors acknowledge a far wider spectrum of gender identities than the "male/female" and "men/women" binary used here, we take a feminist sociological stance in focusing on how the status quo has disadvantaged women (self-identified) in order to reveal power imbalances. This research is in conversation with the broader quantitative data sets that are based upon gender binaries, particularly those that highlight women's historical exclusion from the technology sector, leading to their vulnerability in tech related domains (Wajcman, 2010). Moreover, women are more likely to be victims of a range of cybercrimes (Marcum et al., 2014; Asadullah Khaskheli and Bhuiyan, 2017; Bates, 2017), so research into their cyber resilience cannot be neglected.

2.3. Related research on cyber security education

Students are heavy users of technologies but they do not necessarily receive formal cybersecurity training (Bennett and Maton, 2010; Bennett et al., 2008). In South Africa, the curriculum makes provision for life skills "*… comprising Beginning Knowledge, Creative Arts, Physical Education and Personal and Social Wellbeing*" (Department of Basic Education, South Africa, 2015, p. 8) from Grade R (before school) to Grade 3 however the time allocated to this per week is only 6 hours(for Grade R to 3) and then changes to 4 hours for Grades 4–6. Life Orientation is taught from Grades 7 to 12 for 2 hours per week (Department of Basic Education, South Africa, 2015). In the Life Orientation curriculum, no specific mention is made of cyber security (Department of Education, 2003).

2.4. Gender differences in cyber security

Anwar et al. (Anwar et al., 2017) surveyed 481 company employees to explore their cybersecurity beliefs and behaviours. They report that women reported significantly lower levels of security self-efficacy, whereas Gratian et al. (2018) reported that women were more likely to delay software updates and choose weaker passwords (Gratian et al., 2018). Cain et al. (2018) also revealed that women had lower security knowledge than males in their study (Cain et al., 2018). Halevi et al. (2017) report that the women in their study had a lower sense of self-efficacy when it came to cyber security (Halevi et al., 2017). Anwar et al. recommended that gender sensitive training and intervention programs be designed for cybersecurity awareness (Anwar et al., 2017). This is confirmed by the outcome of a security awareness drive in a secondary school which also detected gender differences (Jin et al., 2018).

However, Chaudhary et al. (2015) study found equal levels of cybersecurity knowledge in their participants, who were all computer science, software engineering or related degree students (Chaudhary et al., 2015). Halevi et al. (2017) also discovered a significant impact of a Computer Science degree on cyber security self efficacy (Halevi et al., 2017). This suggests that gender differences might well have more to do with the gender imbalance in these degree programmes than any other gender-related differences. This is confirmed by Ismailova and Muhametjanova (2016) study (Ismailova and Muhametjanova, 2016).

2.5. Summary

This review demonstrates that women tend not to do computing-related degree programmes and courses. Because most cyber security awareness training occurs within these degree programmes, they will not be exposed to these principles as part of their university education. This, then, means that they feel less aware of cyber security issues, as a demographic. The studies we cite above were carried out in other parts of the world. Here we investigate the state of play in South Africa, as a developing country.

In particular, we want to answer two questions:

RQ1: Is there a difference in cyber security awareness between students doing a computing-related degree and those doing a different kind of degree?

RQ2: Are there gender differences with respect to (1)?

3. Research methodology

3.1. Student project

To explore students' smartphone security and privacy knowledge, the 2016 and 2017 cohort of third year computer science students doing a compulsory Human Computer Interaction (HCI) course at the University of the Western Cape (UWC) in Cape Town were tasked to be researchers. The students were instructed, as a research project, to envisage being employed by a large smartphone company. The company wanted to determine whether smartphone users were aware of smartphone security and privacy issues. We asked the student team to carry out a small research project the better to understand users' security- and privacy-related smartphone experiences. Their fictional company employer "*expected*" the team to write a report based on their findings. In particular, the students were instructed to situate their findings within the current literature and then make suggestions on how the company should design the phone interface in order to improve awareness of security and privacy issues.

Each student team member was asked to find two smartphone owners (older than 18 years and not in their class) to interview. One should *not* have studied computer science or a related subject and the other had previously or currently studied computer science. They were instructed to conduct an interview with their participants, using a predefined questionnaire consisting of 65 questions. For the rest of this report, all participants in the former category will be referred to as: *non-Computer Science* (NCS) and the latter as *Computer Science* (CS) participants.

To train students in carrying out ethical research, they were instructed to ask the potential participant for their consent to be interviewed and to sign a form to confirm that: (1) the participant had read and understood the purpose of the questionnaire; (2) he or she was free to withdraw their participation without providing reasons; (3) he or she would not provide any security-related information to the interviewer and finally (4) granted permission for the information they provided to be used for research purposes (including reports, publications and presentations) with strict preservation of anonymity. Ethical clearance for this research was obtained from the university's research committee.

The aim of the student research project was not only to train students in ethical research but also to make the student researchers themselves more aware of security and privacy issues—the majority of whom are also smartphone owners. Furthermore, since the research was team-based, students also learned how to function within a team and, by implication, how to collaborate, organise team meetings and write a team report.

The data the student teams collected over the 2016–2017 period was combined to answer the following research questions: (1) does a computer science specific education improve cyber resilience, and (2) are there gender differences with respect to (1)?

Quantitative analysis using SAS® (SAS Institute Inc, 2017) was carried out on the data set and also on the following groupings: gender and CS background. The open-ended questions provided additional information that was post-coded and analysed quantitatively.

4. Results

4.1. Descriptive background

In 2016, the student researchers interviewed 100 students (51 CS and 49 NCS students) and in 2017, 152 students (76 CS and 76 NCS) were interviewed. The total number of observations is thus 252.

Forty-one percent of the participants were women—24% of the CS participants and 57% of NCS participants. Most completed their school-leaving certificates in cities (61%) with 39% completing their schooling in small towns or rural areas. On average, the participants had been using smartphones for 5.3 years in the 2016 cohort, and 6.6 years in the 2017 cohort (minimum 0 and maximum 20 years). Most (77%) always kept their mobile phones within reach.

Significantly more men than women took CS as a subject (Chi-sq = 28.06, $P < 0.0001$). This was true for both 2016 and 2017 cohorts, and has been the case for several years now at UWC. This tendency was also experienced at another university in South Africa where the number of women students studying towards a degree in IT dropped from 58 in 2000 to 14 in 2012 (Pretorius et al., 2015).

4.2. Gender as well as CS exposure

When considering gender, as well as CS background separately, it was found that significantly more of the CS-men (78%) versus all others (CS-women 65%, NCS-women 58% and NCS-men 55%) felt that there were security/privacy issues when using PayPal for payments (Chi-sq = 19.1, p = 0.0040). Significantly fewer NCS-men felt that there was no security risk when using online shopping (Chi-sq = 13.6, p = 0.0346) (see Table 2).

More of the CS students (CS-men 48% and the CS-women 42%), when compared to the NCS-students (NCS-women 27% and NCS-men 25%) were aware of privacy/security risks when using BitTorrent (Chi-sq = 29.88, $p < 0.0001$). It was found that more of the CS students (CS-men 39% and the CS-women 43%) when compared to the NCS students (NCS-women 24% and NCS-men 27%) were aware of privacy/security risks when using Bitcoin (Chi-sq = 22.37, p = 0.0010).

When considering gender, as well as CS background, it was found that more of the CS students (CS-men 51% and the CS-women 62%), as compared to the NCS students (NCS-women 27% and NCS-men 37%) understood what “encryption” meant (Chi-sq = 25.651, p = 0.0003) (see Table 3). Furthermore, it was found that more of the CS students (CS-men 64% and the CS-women 55%), as compared to the NCS students (NCS-women 37% and NCS-men 33%), knew how to identify phishing attempts (Chi-sq = 18.18, p = 0.0004).

It seems as if the majority of the CS-men and some of the CS-women find *security advice on the Internet* whereas the NCS-women tend to get the advice by *word of mouth*. Both groups use the Internet, word of mouth, public media and combinations thereof to get security advice (see Figure 4).

Apart from using a PIN (Personal Identification Number) or password, students were in general not concerned about security around friends or family. Most of the students were quite happy to share their passwords with family or friends. More of the women—NCS-women (81%) and CS-women (71%))—compared to the men—NCS-men (59%) and CS-men (65%)—did so and only a few regretted it (see Table 4).

There seems to be very little difference between the device behaviours of the different groups (see Table 5). However, slightly more women kept records of their Phone's IMEI (International Mobile

Table 2. Respondent's perceived mobile phone security or privacy issues.

Are there any security/privacy issues when using:	CS-Women (%) (n = 31)	CS-Men(%) (n = 96)	NCS-Women (%) (n = 71)	NCS-Men (%) (n = 53)	Gender differences in CS/NCS Chi-sq, p-value
Social networking sites	97	92	86	92	Chi-sq = 7.7, p = 0.2630
WhatsApp	84	70	62	58	Chi-sq = 7.4, p = 0.2817
Internet searches	55	65	61	58	Chi-sq = 10.7, p = 0.0972
Online Banking	84	85	77	79	Chi-sq = 6.9, p = 0.3269
PayPal	65	78	58	55	Chi-sq = 19.1, p = 0.0040*
GPS/Google Maps	58	55	45	45	Chi-sq = 8.3, p = 0.2172
Health related apps	52	49	37	45	Chi-sq = 4.7, p = 0.5891
Email	90	83	72	83	Chi-sq = 8.0, p = 0.2396
Online shopping	77	82	75	68	Chi-sq = 13.6, p = 0.0346*
Dating sites	61	69	63	68	Chi-sq = 3.4, p = 0.7524
Uber (taxi services)	57	46	51	44	Chi-sq = 5.5, p = 0.4859
Bit Torrent	42	48	27	25	Chi-sq = 29.9, p < 0.0001*
Bit Coins	43	39	24	27	Chi-sq = 22.4, p = 0.0010*
Passport style photo as a profile picture	58	53	51	51	Chi-sq = 0.5, p = 0.9094

* Significant at a 5% level of significance.

Table 3. Security awareness.

	CS-Women (%) (n = 31)	CS-Men (%) (n = 96)	NCS-Women (%) (n = 71)	NCS-Men (%) (n = 53)	Gender differences in CS/NCS Chi-sq, p-value
Do you ever encrypt data on your mobile phone?	32	40	27	26	Chi-sq = 4.2, p = 0.2440
Could explain what encryption is	62	51	27 (n = 66)	37	Chi-sq = 25.7, p = 0.0003*
Could identify phishing attempts	55	64	37	33	Chi-sq = 18.2, p = 0.0004*
Thinks public media provides helpful security advice	29	25	15	26	Chi-sq = 6.4, p = 0.7041
Thinks social media provides helpful security advice	63	53	46	45	Chi-sq = 8.8930, p = 0.4472

* Significant at a 5% level of significance.

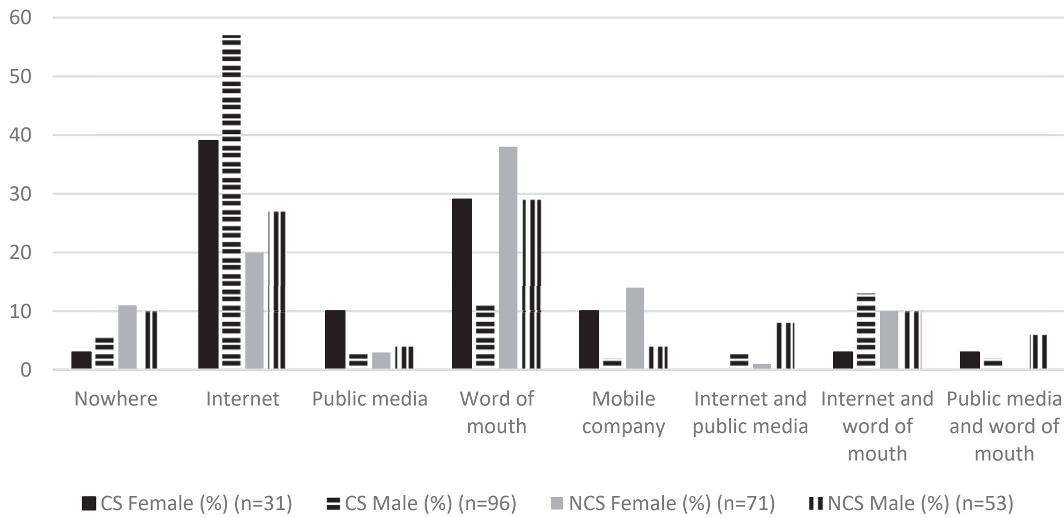

Figure 4. Where security advice is found.

Table 4. Password behaviour.

	CS-Women (%) (n = 31)	CS-Men (%) (n = 96)	NCS-Women (%) (n = 71)	NCS-Men (%) (n = 53)
Use PIN/password	71	84	79	72
Share password	71	65	81	59
Shared password and regretted it	13	14	17	19
Believe it is easy to bypass their smartphone's access control mechanism	20	26	37	31
Hide password when unlocking phone at friends	16	23	23	25
Can protect one's privacy on a mobile phone	60	60	43	53

Table 5. Behaviour in terms of the device.

	CS-Women (%) (n = 31)	NCS-Women (%) (n = 71)	CS-Men (%) (n = 96)	NCS-Men (%) (n = 53)	Gender differences in CS/NCS Chi-sq, p-value
Do delete Apps from phone	65	66	78	70	Chi-sq = 9.7, p = 0.3189
Install system updates and upgrades	74	73	78	74	Chi-sq = 1.5, p = 0.9569
Have a record of the phone's IMEI number	52	48	49	42	Chi-sq = 4.9, p = 0.1758
Know how to lock or wipe phone when stolen or lost	45	23	47	36	Chi-sq = 13.7, p = 0.0335*
Take precautions when selling or giving phone away	71	59	81	74	Chi-sq = 10.0, p = 0.0186*
Back-up data on phone regularly	71	35	53	53	Chi-sq = 12.2, p = 0.0067*
Do you have any anti-virus software on your phone?	35	30	41	40	Chi-sq = 2.5, p = 0.4688

* Significant at a 5% level of significance.

Equipment Identity**)** number than their male counterparts. Very few had anti-virus software on their phones. More of the CS students (CS-men 47% and the CS-women 45%), as compared to the NCS students (NCS-women 23% and NCS-men 36%), knew how to lock or wipe their phones when lost or stolen (Chi-sq = 13.7, p = 0.0335). More of the men and CS-women (CS men 81%, NCS-men 74% and the CS-women 71%), as compared to the NCS-women (NCS-women 59%), took action when selling or giving their phones away (Chi-sq = 10.0, p = 0.0186). More of the CS-women (71%), as compared to the rest (NCS-women 35%, CS-men 53% and NCS-men 53%), regularly backed up the data on their phones (Chi-sq = 12.2, p = 0.0067).

Very few of the smartphone users offered security advice to fellow users (see Table 6). However significantly more of the CS students (CS-men 38% and the CS-women 35%), as compared to the NCS students (NCS-women 17% and NCS-men 15%), offered security advice to other smartphone users (Chi-sq = 21.1, p = 0.0018).

Some of the students knew that they could be held liable for tweets even if it did not originate from them. More men seemed to make friends online than women. However, when combining the CS and NCS groups, significantly more of the men (76%), as compared to women (56%), reported having made a friend online (Chi-sq = 11.45, p = 0.0095).

In the next section the data will be discussed in terms of how it answers the research questions.

5. Discussion

The first research question posed was (RQ1) *Is there a difference in cyber security awareness between students doing a computing-related degree and those doing a different kind of degree?* It is clear that a computer science education does indeed improve awareness of smartphone security and privacy issues, and precautions to be taken. Table 3 demonstrates a clear positive impact of a computing science education in this respect. More of the CS students understood the risks of BitTorrent and Bitcoin, understood the term "*encryption*", and felt able to identify phishing messages. The majority of the CS-men, and some of the CS-women, found security advice on the Internet and tended to offer security advice to other smartphone users.

The second question posed was (RQ2) *Are there gender differences?* The CS-women were more resilient than all students (men and women) doing NCS degrees, demonstrating the value of a CS education, regardless of gender. Indeed, the general awareness trends shown in Table 2 demonstrate a clear difference between CS (left two columns) and NCS students (right two columns) across the board. It is interesting to note that more of the CS-women regularly made backups of the data on their phones, perhaps because they perceive that they are easier targets for theft? Suggestions for future research could include a more qualitative approach and doing in-depth interviews to uncover reasons. Furthermore, fewer women reported having made a friend online. This could be

Table 6. Social behaviour in terms of mobile usage.

	CS-Women (%) (n = 31)	NCS-Women (%) (n = 71)	CS-Men (%) (n = 96)	NCS-Men (%) (n = 53)	Gender differences in CS/NCS, Chi-sq, p-value
Offer security advice to other smartphone users	35	17	38	15	Chi-sq = 21.1*, p = 0.0018
Can be held liable for re-tweeting, liking or sharing tweets	58	48	44	40	Chi-sq = 8.5, p = 0.4892
Made a friend online	58	56	78	73	Chi-sq = 15.6, p = 0.0752

* Significant at a 5% level of significance.

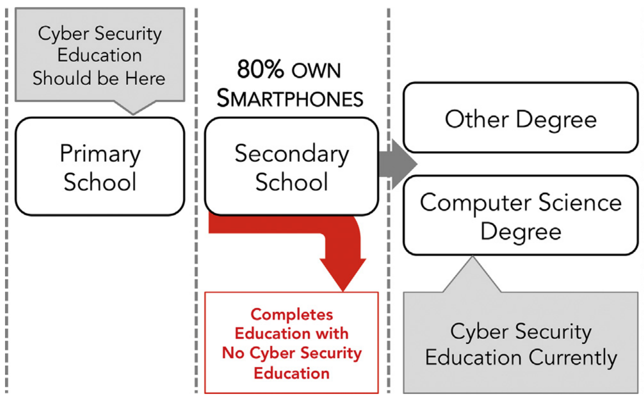

Figure 5. Reconsidering the South African security education approach.

because of women's heightened sense of vulnerability. Yet, as demonstrated earlier, being content with this situation is not an option. The fact that fewer women do computing subjects at school, and that fewer women study CS at university (van Broekhuizen and Spaull, 2017) effectively leads to the situation where fewer women benefit from heightened cyber security awareness.

It does seem as if a CS education improves awareness, and it does so for both genders. This confirms findings by Darkish et al. that students with a technology or science background were less vulnerable to phishing attacks (Darkish et al., 2012). Moreover, Gratian et al. found that university students (aged 18–25) and students majoring in the humanities would benefit from security training (Gratian et al., 2018).

The discouraging conclusion is that upcoming generations of South Africans who do not study CS will have insufficient awareness of privacy and security issues, and will, as a consequence, be more vulnerable to cyber-attacks. Moreover, women will be disproportionately affected. The South African educational system can no longer leave it to Universities to raise cyber security awareness. Fundamental cyber security life skills should be taught at primary school, delivered to all pupils, ensuring that awareness is raised in all genders equally. Cyber security awareness and resilience is too important for any government to leave to chance (Renaud et al., 2018).

Figure 5 shows where cyber security education is currently being delivered (at University), and where it ought to be delivered (at Primary School). Moving it earlier will ensure that when people get their first smartphone they will already have sufficient awareness and skills to secure their new devices. It is also likely to remove the gender differences we observed in our study.

6. Conclusion

This study investigated smartphone cyber security awareness amongst students at a South African university. We confirmed the benefit of a CS education in this respect: a heartening yet disappointing finding. The former because this means the university is doing a great job of improving awareness in CS teaching. The latter because anyone who is not enrolled for a CS course at university is not getting the requisite information to be able to improve their own cyber resilience. This means that the South African approach to cyber security awareness is failing, in terms of producing a cyber resilient population.

Moreover, the extant imbalance between genders in CS degrees means that South African women are more vulnerable to cyber-attacks. This suggests an urgent need to teach cyber security principles much earlier in the educational system so that the cyber resilience of all South Africans, regardless of gender, can be assured.

Declarations

Author contribution statement

I. Venter: Conceived and designed the experiments; Performed the experiments; Contributed reagents, materials, analysis tools or data; Wrote the paper.

R. Blignaut: Conceived and designed the experiments; Analyzed and interpreted the data; Contributed reagents, materials, analysis tools or data; Wrote the paper.

K. Renaud: Conceived and designed the experiments; Contributed reagents, materials, analysis tools or data; Wrote the paper.

A. Venter: Contributed reagents, materials, analysis tools or data; Wrote the paper.

Funding statement

This work was supported by the National Research foundation [grant numbers 103627, 109041] and the Research Committee of the University of the Western Cape [grant number 2013/06/08; 05/01/33].

Competing interest statement

The authors declare no conflict of interest.

Additional information

No additional information is available for this paper.

Acknowledgements

This work was supported by the National Research foundation [grant numbers 103627, 109041]; and the Research Committee of the University of the Western Cape [grant numbers 2013/06/08; 05/01/33].

References

Akamai Technologies, 2017. State-of-the-Internet. Retrieved September 18, 2018, from Akamai: https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q1-2017-state-of-the-internet-connectivity-report.pdf.
Alozie, N.O., Akpan-Obong, P., 2017. The digital gender divide: confronting obstacles to women's development in Africa. Dev. Policy Rev. 35 (2), 137–160.
Anwar, M., He, W., Ash, I., Yuan, X., Li, L., Xu, L., 2017. Gender difference and employees' cybersecurity behaviors. Comput. Hum. Behav. 69, 437–443.
Asadullah Khaskheli, Y.J., Bhuiyan, M.A., 2017. M-commerce and mobile apps: opportunities for SMEs in developing countries. J. Int. Bus. Res. Mark. 2 (2), 20–23.
Bates, S., 2017. Revenge porn and mental health: a qualitative analysis of the mental health effects of revenge porn on female survivors. Fem. Criminol. 12 (1), 22–42.
Beede, D., Julian, T., Langdon, D., McKittrick, G., Khan, B., Doms, M., 2011. Office of the Chief Economist. Retrieved 10 12, 2019, from Women in STEM: A Gender Gap to Innovation : https://files.eric.ed.gov/fulltext/ED523766.pdf.
Beger, G., Sinha, A., 2012. South African Mobile Generation:: Study on South African Young People on Mobiles. Retrieved August 09, 2019, from UNICEF: https://www.unicef.org/southafrica/resources_10782.html.
Bennett, S., Maton, K., 2010. Beyond the 'digital natives' debate: towards a more nuanced understanding of students' technology experiences. J. Comput. Assist. Learn. 26 (5), 321–331.
Bennett, S., Maton, K., Kervin, L., 2008. The 'digital natives' debate: a critical review of the evidence. Br. J. Educ. Technol. 39 (5), 775–786.

Businesstech, 2019. News. Retrieved August 08, 2019, from How old kids are when they receive their first cellphone – South Africa vs the rest of the world: https://businesstech.co.za/news/mobile/215997/how-old-kids-are-when-they-receive-their-first-cellphone-south-africa-vs-the-rest-of-the-world/.
Cain, A.A., Edwards, M.E., Still, J.D., 2018. An exploratory study of cyber hygiene behaviors and knowledge. J. Inf. Secur. App. 42, 36–45.
Carr, N.G., 2003. IT doesn't matter. Educ. Rev. 38, 24–38.
Chaudhary, S., Zhao, Y., Berki, E., Valtanene, J., Li, L., Helenius, M., Mystakids, S., 2015. A cross-cultural and gender-based perspective for online security: exploring knowledge, skills and attitudes of higher education students. IADIS Int. J. WWW/Internet 13 (1).
Chigona, W., Mudavanhu, S.L., Siebritz, A., Amerika, Z., 2016. Domestication of free Wi-Fi amongst people living in disadvantaged communities in the Western Cape province of South Africa. In: Proceedings of the Annual Conference of the South African Institute of Computer Scientists and Information Technologists. ACM (p. Paper 9).
Chinyamurindi, W.T., Louw, G.J., 2010. Gender differences in technology acceptance in selected South African companies: implications for electronic learning. SA J. Hum. Resour. Manag. 8 (1), 1–7.
Choi, S.Y., Ting, K.F., 2008. Wife beating in South Africa: an imbalance theory of resources and power. J. Interpers Violence 23 (6), 834–852.
Cockburn, H., 2019. Schools to Teach Children about Fake News and 'confirmation Bias', Government Announces. Retrieved August 8, 2019, from The Independent: https://www.independent.co.uk/news/education/education-news/fake-news-schools-education-online-risks-confirmation-bias-damian-hinds-government-a9004516.html.
Darkish, A., El Zarka, A., Aloul, F., 2012. Towards understanding phishing victims' profile. Comput. Syst. Ind. Inf. 1–5.
De Lange, M., Von Solms, R., 2012. An E-Safety Educational Framework in South Africa. South African Telecommunications Networks and Applications. George, South Africa. Paper 53).
Department of Basic Education South Africa, 2015. National Policy Pertaining to the Programme and Promotion Requirements of the National Curriculum Statement Grades R - 12. Retrieved July 16, 2019, from Basic Education: https://www.education.gov.za/Portals/0/Documents/Policies/NATIONAL%20POLICY%20PERTAINING%20TO%20THE%20PROGRAMME%20AND%20PROMOTION%20REQUIREMENTS%20OF%20THE%20NCS.pdf?ver=2016-01-18-091032-337.
Department of Education, 2003. Life Orientation Curriculum. Retrieved 07 20, 2019, from Education. https://www.education.gov.za/Portals/0/CD/SUBSTATEMENTS/Life%20Orientation.pdf?ver=2006-08-31-121627-000.
Dlamini, Z., Modise, M., 2013. Cyber security awareness initiatives in South Africa: a synergy approach. Case Stud. Inf. Warf. Secur. Res. Teach. Stud, p.1. In: Warren, M. (Ed.), Case Studies in Information Warfare and Security for Researchers, Teachers and Students. Academic Conferences and Publishing International Ltd, Reading, United Kingdom, pp. 1–22.
Education and Training Foundation, 2019. Functional Skills Standards and Curriculum. Retrieved August 8, 2019, from Excellence Gateway Toolkits: https://toolkits.excellencegateway.org.uk/functional-skills-starter-kit/section-3-developing-effective-practice/functional-skills-standards-and-curriculum.
European Platform of Women Scientists, 2016. The Women in IT Scorecard. Retrieved August 9, 2019, from The Tech Patnership skills for the digital economy: https://epws.org/women-in-it-scorecard/.
Fowler, K., 2016. Data Breach Preparation and Response: Breaches Are Certain, Impact Is Not. Elsevier, Syngress, Cambridge.
Gratian, M., Bandi, S., Cukier, M., Dykstra, J., Ginther, A., 2018. Correlating human traits and cyber security behavior intentions. Comput. Secur. 73, 345–358.
Halevi, T., Memon, N.D., Levis, J., Kumaraguru, P., Arora, S., Dagar, N., Chen, J., 2017. Cultural and psychological factors in cyber security. J. Mob. Multimed. 13 (1 & 2), 43–56.
Hanus, B., Wu, Y.A., 2016. Impact of users' security awareness on desktop security behavior: a protection motivation theory perspective. Inf. Syst. Manag. 33 (1), 2–16.
Ismailova, R., Muhametjanova, G., 2016. Cyber crime risk awareness in Kyrgyz Republic. Inf. Secur. J. A Glob. Perspect. 25 (1-3), 32–38.
ITU, 2018a. Committed to Connecting the World. Retrieved April 17, 2018, from Internet users by region and country, 2010-2016: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/treemap.aspx.
ITU, 2018b. ICT Facts and Figures 2017. Retrieved April 17, 2018, from International Telecommunications Union: https://www.itu.int/en/itu-d/statistics/documents/facts/ictfactsfigures2017.pdf.
Jin, G., Tu, M., Kim, T.H., Heffron, J., White, J., 2018. Evaluation of game-based learning in cybersecurity education for high school students. J. Educ. Learn. 12 (1), 150–158.
Kortjan, N., Von Solms, R., 2014. A conceptual framework for cyber-security awareness and education in SA. S. Afr. Comput. J. 52 (1), 29–41.
Krebs, B., 2017. 4 Years after Target, the Little Guy Is the Target. Retrieved July 8, 2019, from Krebs on Security: https://krebsonsecurity.com/2017/12/4-years-after-target-the-little-guy-is-the-target/.
Langen, T.T., 2005. Gender power imbalance on women's capacity to negotiate self-protection against HIV/AIDS in Botswana and South Africa. Afr. Health Sci. 5 (3), 188–197.
Livingston, S., Nandi, A., Banaji, S., Stoilova, M., 2017. Young Adolescents and Digital media: Uses, Risks and Opportunities in Low-And Middle-Income Countries: a Rapid Evidence Review. Gage, London, UK.
Marcum, C.D., Higgins, G.E., Ricketts, M.L., 2014. Juveniles and cyber stalking in the United States: an analysis of theoretical predictors of patterns of online perpetration. Int. J. Cyber Criminol. 8 (1).
Mayer, A., 2014. Smartphones Becoming Prime Target for Criminal Hackers. Retrieved April 24, 2018, from CBC News: http://www.cbc.ca/news/technology/smartphones-becoming-prime-target-for-criminal-hackers-1.2561126.
Newzoo, 2017. Top 50 Countries by Smartphone Users and Penetration. Retrieved from Insights: https://newzoo.com/insights/rankings/top-50-countries-by-smartphone-penetration-and-users/.
Nias, J., Southworth, G., Campbell, P., 2005. Whole School Curriculum Development in the Primary School. Routledge.
North, D., Johnston, K., Ophoff, J., 2014. The Use of Mobile Phones by South African University Students, 11. Issues in Informing Science & Information Technology.
Numbeo, 2018. Prices by Country of Internet (60 Mbps or More, Unlimited Data, Cable/ADSL). Retrieved September 18, 2018, from Numbeo: https://www.numbeo.com/cost-of-living/prices_by_country.jsp?displayCurrency=USD&itemId=33.
Olapido, T., 2015. Cyber-crime Is Africa's 'next Big Threat', Experts Warn. Retrieved July 08, 2019, from BBC News: http://www.bbc.co.uk/news/world-africa-34830724.
Organisation for Economic Co-operation and Development, 2009. Pisa 2006 Technical Report. Programme for International Student Assessment. OECD. Retrieved April 22, 2018, from Organisation for Economic Co-operation and Development 2009: https://www.oecd.org/pisa/data/42025182.pdf.
Percy, R., Timbs, J., 2019. The Mirror of Literature, Amusement, and Instruction, 5. Wentworth Press.
Pew Research Centre, 2018. Smartphone Ownership on the Rise in Emerging Economies. Retrieved September 26, 2018, from Global attitudes and trends: http://www.pewglobal.org/2018/06/19/2-smartphone-ownership-on-the-rise-in-emerging-economies/.
Porter, G., 2016. How mobile Phones Are Disrupting Teaching and Learning in Africa. Retrieved August 9, 2019, from The Conversation: https://theconversation.com/how-mobile-phones-are-disrupting-teaching-and-learning-in-africa-59549.
Pretorius, H.W., Mawela, T., Strydom, I., De Villiers, C., Johnson, R.D., 2015. Continuing the discourse of women in information techology A South African perspective. Gend. Technol. Dev. 19 (3), 1–24.
Renaud, K.V., Blignaut, R.J., Venter, I.M., 2016. Smartphone owners need security advice. How can we ensure they get it?. In: International Conference on Information Resources Management, (P. Paper 60). Cape Town.
Renaud, K., Flowerday, S., Warkentin, M., Orgeron, C., Cockshott, W., 2018. Is the responsibilization of the cyber security risk reasonable and judicious? Comput. Secur. 78, 198–211.
SAS Institute Inc, 2017. SAS/STAT 14.3 User's Guide. SAS Institute Inc, Cary, NC, USA.
Siponen, M.T., 2001. Five dimensions of information security wareness. Comput. Soc. 31 (2), 24–29.
Statista, 2019. Mobile Internet Traffic as Percentage of Total Web Traffic as of January 2018, by Country. Retrieved August 09, 2019, from Statista: https://www.statista.com/statistics/430830/share-of-mobile-internet-traffic-countries/.
Sutton, J., 2011. E-safety in Primary Schools. Retrieved August 08, 2019, from Teach Primary: https://www.teachprimary.com/learning_resources/view/e-safety-in-primary-schools.
The World Bank, 2016. World Development Report: Digital Dividents. Retrieved 03 27, 2018, from Worldbank.org: https://documents.worldbank.org/curated/en/896971468194972881/pdf/102725-PUB-Replacement-PUBLIC.pdf.
UNESCO Education Sector, 2017. Cracking the code: girls' and women's educaiton in science, technology, engineering and mathematics (STEM). In: Conference:UNESCO International Symposium and Policy Forum. UNESCO, Paris, France.
van Broekhuizen, H., Spaull, N., 2017. The 'martha effect': the compounding female advantage in South Africa. In: Biennial Conference of the Economic Society of South Africa. Rhodes University, Grahamstown, South Africa.
von Solms, S., Von Solms, R., 2014. Towards cyber safety education in primary schools in Africa. In: Proceedings of the Eighth International Symposium on Human Aspects of Information Security & Assurance. HAISA 2014), pp. 185–197.
Wajcman, J., 2010. Feminist theories of technology. Camb. J. Econ. 34 (1), 143–152.
Waldron, J., 2006. Safety and security. Neb. Law Rev. 85, 454.
World Economic Forum, 2017a. The Future of Jobs Employment, Skills and Workforce Strategy for the Fourth Industrial Revolution. Retrieved 04 22, 2018, from Global Challenge Insight Report: http://www3.weforum.org/docs/WEF_Future_of_Jobs.pdf.
World Economic Forum, 2017b. Accelerating Gender Parity in the Fourth Industrial Revolution: an Agenda for Leaders to Shape the Future of Education, Gender and Work. Retrieved April 24, 2018, from World Economic Forum: https://www.weforum.org/whitepapers/accelerating-gender-parity-in-the-fourth-industrial-revolution.